AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on page 1, line 14, with the following rewritten paragraph:

-- This application claims priority to U.S. Provisional Patent Application No. 60/151,531 entitled “SYSTEM AND METHOD FOR PROVIDING COMPUTER SECURITY” filed August 30, 1999, which is incorporated herein by reference for all purposes._ ~~, and to~~ U.S. Patent Application No. 09/615,697 entitled "SYSTEM AND METHOD FOR COMPUTER SECURITY" filed July 14, 2000, ~~which~~ is incorporated herein by reference for all purposes.--

Please replace the paragraph beginning on page 1, line 10, with the following rewritten paragraph:

--This application is related to co-pending U.S. Patent Application No. 09/651,303 ~~No. ______________ (Attorney Docket No. RECOP012~~ entitled EXTENSIBLE INTRUSION DETECTION SYSTEM filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/651,854 ~~No. ___________ (Attorney Docket No. RECOP013)~~ entitled SYSTEM AND METHOD FOR USING LOGIN CORRELATIONS TO DETECT INTRUSIONS filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/651,434 ~~No. ___________ (Attorney Docket No. RECOP014)~~ entitled SYSTEM AND METHOD FOR USING SIGNATURES TO DETECT COMPUTER INTRUSIONS filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/651,304 ~~No. ___________ (Attorney Docket No. RECOP015)~~ entitled SYSTEM AND METHOD FOR ANALYZING FILESYSTEMS TO DETECT INTRUSIONS filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/651,306 ~~No. __________ (Attorney Docket No. RECOP016)~~ entitled SYSTEM AND METHOD FOR DETECTING BUFFER OVERFLOW ATTACKS filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/654,347 ~~No. __________ (Attorney Docket No. RECOP017)~~ entitled SYSTEM AND METHOD FOR USING TIMESTAMPS TO DETECT ATTACKS filed concurrently herewith, which is incorporated herein by reference for all purposes.--

Please replace the paragraph beginning on page 88, line 1, with the following rewritten paragraph:

--Figure 6 illustrates a rule-based system and processes used in some embodiments to detect computer intrusions using a hybrid approach in which both forward chaining and backward chaining are used. Two categories of rule-based systems are those that use *forward-chaining* and those that use *backward-chaining*. Systems that use forward-chaining (602) start with each incoming fact (604) and generate all inferences (606) resulting from the addition of that fact to the knowledge base (608), thereby producing all conclusions that are supported by the available facts. Systems that use backwards-chaining (610) start with a goal (614) and search for facts that support that goal, producing a structure of subgoals (612). Both approaches have the potential for substantial *over-generation*: computing inferences that are never used (forward-chaining) or hypothesizing sub-goals for which there is no support (backward-chaining). The forward- and backward-chaining approaches are analogues of bottom-up and top-down parsing in compiler technology.--

Please replace the paragraph beginning on page 88, line 11, with the following rewritten paragraph:

--Because of the complexity of the data, an embodiment of the invention may use a hybrid approach in its analysis engine (616). Incomplete data presents serious difficulties for a backward-chaining. For example, it becomes impossible to falsify (discard) a sub-goal when any of the supporting data is not found. Similarly, for forward-chaining, missing data blocks the formation of needed inferences. The system of the invention uses forward chaining to generate inferences, but limits the length of the chains (620, 622, 624, and 626). The chains are limited to simple combinations that are easily found along a dimension; e.g., a linear sequence of events within a login session, or a sequence of attempted logins from the same host. Inferences that match sub-goals (628) then trigger backwards chaining (620, 622, and 630) from that sub-goal's potential parents into other sub-goals (632). Backward chaining handles combining events that are more separated or of flexible ordering, and for postulating missing events.--